

Державний вищий навчальний заклад
«Донецький національний технічний університет»
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

В.о. першого проректора

_____ Леонід БАЧУРІН

«_____» _____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОНД 2.14 (ОК27) Архітектура систем захисту інформації (КЗСІ)

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність (ості) _____ 125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма _____ Кібербезпека

(назва освітньої програми, для обов'язкових дисциплін)

Мова навчання: українська

Робоча програма навчальної дисципліни Архітектура систем захисту інформації
(повна назва дисципліни)
для здобувачів вищої освіти за спеціальністю 125 Кібербезпека.

«27» грудня 2023 року. – 7 с.

Розробник: Дорогий Ярослав Юрійович, д.т.н., професор кафедри прикладної математики та інформатики ДВНЗ «ДонНТУ».

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики.

Протокол № 13 від «27» грудня 2023 р.

Завідувач кафедрою прикладної математики та інформатики ДВНЗ «ДонНТУ»

27.12.2023 р.

(підпис)

(Наталія МАСЛОВА)

(прізвище та ініціали)

Схвалено науково-методичною комісією з галузі знань 12 Інформаційні технології
(шифр, назва)

Протокол № 1 від «15» січня 2024 р.

Голова

(підпис)

(Євген БАШКОВ)

(прізвище та ініціали)

15.01.2024 р.

1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	Обов'язкова дисципліна циклу професійної підготовки	
Обсяг в кредитах ЄКТС	5	-
Обсяг в годинах за навчальним планом, разом:		-
в тому числі:	150	
лекції:	32	-
практичні заняття:	-	-
лабораторні заняття:	32	-
семінари:	-	-
самостійна робота:	86	-
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Дорогий Ярослав Юрійович, yaroslav.dorohyi@donntu.edu.ua , https://donntu.edu.ua/kitaer/pmi	

Передумови для вивчення дисципліни: успішному вивченню дисципліни «Архітектура систем захисту інформації» сприяє попереднє опанування таких дисциплін як «Основи інформаційної безпеки», «Захист операційних систем», «Керування ризиками інформаційної безпеки», «Безпека та захист операційних систем».

2. Мета вивчення навчальної дисципліни

Метою викладання навчальної дисципліни є формування системи теоретичних знань і практичних навичок з основ теорії, методів і засобів розробки архітектури комплексних систем захисту інформації.

Компетентності:

ЗК01. Здатність застосовувати знання у практичних ситуаціях

ФК05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

ПРН07. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

ПРН12. Розробляти моделі загроз та порушника.

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.

3. Очікувані результати навчання

Результатами опанування дисципліни «Архітектура систем захисту інформації» є наявність базових знань зі спеціальності, здатність застосовувати спеціалізовані програмно-апаратні комплекси та методики в галузі інформаційного захисту.

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання опануванні дисципліною «Архітектура програмних систем захисту інформації»:

- екзамени;
- індивідуальні завдання з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Лр.1	Лр.2	Лр.3	Лр.4	Лр.5	Лр.6	Лр.7	Лр.8	Поточний контроль	Іспит	Максимальний бал
5	5	5	5	5	5	5	5	40	60	100
3	3	3	3	3	3	3	3	24		

Примітка:

- 1) Лр1, Лр2 і т.д лабораторні роботи.
- 2) У чисельнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоечасному виконанні).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену
90-100	Відмінно
74-89	Добре
60-73	Задовільно
0-59	Незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Нормативно-правове забезпечення сфери захисту інформації.

Тема 2. Моделі порушника та загроз для інформації в ІТС.

Тема 3. Політика безпеки ІТС.

Тема 4. Комплексна система захисту інформації. Загальні положення.

Тема 5. Проектування КСЗІ.

Тема 6. Введення в дію КСЗІ.

Тема 7. Державна експертиза КСЗІ.

Тема 8. Супровід КСЗІ.

Тема 9. Системи захисту інформації для різних автоматизованих систем

6.2. Темы лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Лабораторна робота №1 Основні положення інформаційної безпеки держави. Система нормативно-правового та організаційного управління інформаційною безпекою. Міжнародні стандарти та рекомендації в галузі забезпечення інформаційної безпеки.	4	-
2	Лабораторна робота №2 Дослідження структури об'єкту захисту	4	-
3	Лабораторна робота №3 Дослідження структури об'єкту захисту	4	-
4	Лабораторна робота №4 Розробка моделі порушника безпеки інформації	4	-
5	Лабораторна робота №5 Моделі загроз. Класифікації моделі загроз.	4	-
6	Лабораторна робота №6 Складання календарного плану робіт із захисту інформації	4	-
7	Лабораторна робота № 7 Методологія MSAT, що використовується для формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації. Дослідження політики безпеки об'єкту захисту	4	-
8	Лабораторна робота № 8 Протокол випробувань комплексних систем захисту інформації	4	-
...	Усього годин	32	-

6.3. Теми практичних (семінарських) занять
Не передбачено навчальним планом

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Тема 1. Нормативно-правове забезпечення сфери захисту інформації.	6	-
2	Тема 2. Моделі порушника та загроз для інформації в ІТС.	10	-
3	Тема 3. Політика безпеки ІТС.	10	-
4	Тема 3. Комплексна система захисту інформації. Загальні положення.	6	-
5	Тема 4. Проектування КСЗІ.	12	-
6	Тема 5. Введення в дію КСЗІ.	10	-
7	Тема 6. Державна експертиза КСЗІ.	6	-
8	Тема 7. Супровід КСЗІ.	6	-
9	Тема 9. Системи захисту інформації для різних автоматизованих систем	20	-
...	Усього годин	86	-

6.5. Індивідуальні та/або групові завдання
Не передбачено навчальним планом

7. Література

7.1. Основна

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця: ВНТУ, 2018. – 118 с.
2. Гребенніков В. В. Комплексні системи захисту інформації: проектування, впровадження, супровід /В. В. Гребенніков/ Litres, 2019. – 613 с.
3. Конспект лекцій з дисципліни «Архітектура та проектування програмного забезпечення» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Інженерія програмного забезпечення» із спеціальності 121 – «Інженерія програмного забезпечення» / Укл. В. В. Завгородній, К. М. Ялова.– Кам'янське: ДДТУ, 2019.– 144с.
4. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
5. Хорошко В. О. Проектування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць/ Львів: Видавництво Львівської політехніки, 2020. - 320 с.
6. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту: Навч.посіб. /В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін - К.: Ліра-К, 2020. - 554 с.

7.2. Допоміжна

1. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.
2. Горохов С.М. Інформаційна безпека цифрових програмно-керованих АТС: навч. посіб. /С.М. Горохов, В.Г. Кононович, С.В. Стайкуца та ін. - Одеса, 2013. - 244 с.
3. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. –КІПВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

7.3. Методична

1. Схемоконспект лекцій з навчальної дисципліни «Архітектура систем захисту інформації» : ел. навч.-наоч. посіб. для студентів всіх форм навчання галузі знань 12 Інформаційні технології / уклад. Я.Ю. Дорогий, Т.В. Алтухова. – Луцьк : ДонНТУ, 2024 (планується).
2. Методичні вказівки до лабораторних робіт з дисципліни «Архітектура систем захисту інформації» для студентів всіх форм навчання галузі знань 12 Інформаційні технології [Електронне видання] / Я.Ю. Дорогий, Т.В. Алтухова. – ДВНЗ «ДонНТУ», 2024 (планується).

8. Інформаційні ресурси

1. Закон України «Про інформацію»: *поточна редакція від 27.07.2023 р. №2657-XII* / Верховна Рада України. – Офіц. вид. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах»: *поточна редакція від 31.12.2023 р. №80/94-ВР* / Верховна Рада України. – Офіц. вид. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
3. НД ТЗІ 3.7-003-05 Порядок проведення робіт зі створення КСЗІ. – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>